Torsion-point attacks on SIDH-like schemes

Péter Kutas, Christophe Petit

University of Birmingham

7th June 2021

Isogeny-based cryptography

Hard, well-studied number theoretical problems :

- Compute any isogeny between two supersingular elliptic curves
- Compute a degree d isogeny between two supersingular elliptic curves
- Compute the endomorpism ring of a supersingular elliptic curve

These problems seem to be hard even for a quantum computer$\rightarrow$ Isogeny-based cryptography is a viable option for PQC

SIKE

- SIDH -10 years old
- In SIDH you are given extra information : $\phi(P), \phi(Q)$
- Not a well-studied problem
- Natural question : Study this problem in more detail and see whether this can be exploited
- Torsion-point attacks : Active attacks, reduction to endomorphism ring computation, classical and quantum passive attacks

Active attack

- Natural question : can you use static keys in SIDH ; Answer : No
- Galbraith-Petit-Shani-Ti : active attack using malformed torsion points
- Attack model : α is Alice's secret Oracle is given E, E_B, P, Q, E' where $P, Q \in E$ and have order A
- Oracle returns true if $E' \cong E_B/\langle P + \alpha Q\rangle$ otherwise returns false
- Motivation : in SIDH $P = \phi_B(P_A),\ Q = \phi_B(Q_A)$ but Alice cannot check whether this is the case (Alice can check the order of P, Q thus can thwart a trivial attack)
- Store already computed bits, in every iteration get one more bit of the secret
- Countermeasures : Fujisaki-Okamoto, k-SIDH, Jao-Urbanik scheme

Isogeny problem with torsion information

This motivates the study of the follwoing algorithmic problem :

Problem (SSI-T)

Let ϕ be a secret isogeny of degree A between supersingular elliptic curves E_1 and E_2. Suppose that you know $\phi(P_B)$ and $\phi(Q_B)$. Compute ϕ

- Goal : give conditions on the relationship between A, B, p for which we can solve this problem in polynomial time (or at least improve on generic meet-in-the-middle)

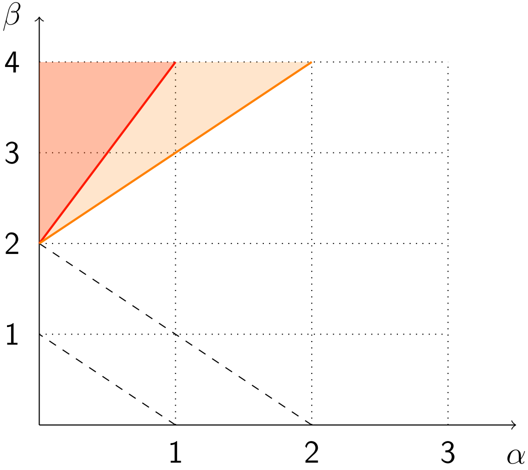
Passive torsion-point attacks

- Find a special endomorphism θ of E_0 and an integer d such that $\tau = \phi \circ \theta \circ \hat{\phi} + [d]$ is computable
- Computing $ker(\tau - d) \cap E_A[A]$ will return $\hat{\phi}$
- How do you find θ ?
- Two types of attacks : 1. $E_0 : y^2 = x^3 + x$, 2. backdoor attack

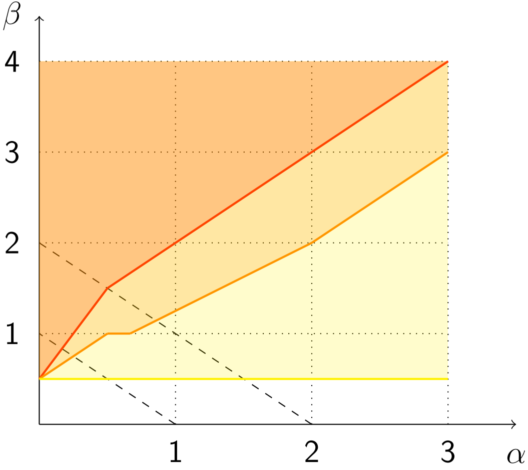
A tale of three equations

- You can compute τ if $\deg(\tau) = Be$ where e is small
- Improvements : instead of B one can have B^2 (using dual information) or B^2p (using the Frobenius isogeny)
- One can look for θ as $ci + bj + aij$
- $A^2(a^2p + b^2p + c^2) + d^2 = Be$
- $A^2(a^2p + b^2p + c^2) + d^2 = B^2e$
- $A^2(a^2p + b^2p + c^2) + d^2 = B^2pe$

Petit 2017



de Quehen, Kutas, Leonardi, Martindale, Panny, Petit, Stange 2021



Main impact of attacks : polynomial-time key recovery when $p \approx AB$ and $B > A^5$

Backdoor attacks

- Can you generate starting curves from which one can solve SSI-T in polynomial time/faster than meet-in-the-middle ?
- Answer : yes
- Whenever $B > A^2$ (the condition is independent of p) then one can generate (A, B)-backdoor curves with a polynomial-time key recovery
- When $A \approx B$ then one can generate backdoor curves which beat current attacks
- Backdoor curves are hard to distinguish from random curves

Quantum hidden shift attack

- SIDH does not admit a similar group action as CSIDH thus is not vulnerable to Kuperberg's subexponential algorithm
- Alternative group action : let O be the endomorphism ring of E_0, then $(O/AO)*$ acts on curves of distance A from E_0
- Let $E_A = E/\langle A \rangle$ be the secret curve of distance A
- Then $\theta * E_A := E = \langle \theta(A) \rangle$; If one chooses a suitable subgroup of $(O/AO)^*$ then this action is free and transitive and one can apply a Kuperberg-style attack
- The group action is computable whenever $B > pA^4$
- Worse than previous attack but shows previously unknown structure of the problem

Past, Present,Future

- Torsion-point attacks-5 years
- Impact on balanced SIDH : cannot reuse keys
- Passive attacks do not impact SIKE parameters
- Cryptoanalysis picture is much clearer (or less clear from a different perspective)
- (small) breakthrough : don't use unbalanced variants !
- don't trust starting curves coming from an unknown source
- Future : Combine classical attack with quantum hidden shift attack